EXHIBIT A

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In re: Clearview AI, Inc. Consumer Privacy Litigation	)	Civil Action No. 1:21-cv-00135

AMICUS CURIAE BRIEF OF CENTER ON PRIVACY & TECHNOLOGY IN SUPPORT OF PLAINTIFFS' OPPOSITION TO CLEARVIEW DEFENDANTS' MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Statutes

Other Authorities

STATEMENT OF INTEREST

The Center on Privacy & Technology at Georgetown Law (the Center) is a think tank which investigates ways in which modern surveillance technologies expand the government's ability to monitor and track individuals. The Center has extensively researched and published reports on a wide range of issues raised by facial recognition technology, such as how algorithmic biases disproportionately affect people of color and how police officers' misuse of the technology increases the risk of false identification. The Center files this amicus brief to provide the Court insights on the ways in which the Illinois Biometric Information Privacy Act (BIPA) mitigates the harms of facial recognition technology and protects Illinois residents' rights to privacy and free expression.

INTRODUCTION AND SUMMARY OF ARGUMENT

The Illinois Biometric Information Privacy Act (BIPA) prohibits private entities like Clearview AI from collecting and disseminating a person's biometric information without first obtaining that person's informed consent. 740 ILCS 14/15(b), (d). In violation of BIPA, Clearview AI has compiled Illinois residents' biometric information and disclosed that information to law enforcement agencies without providing notice to residents, let alone obtaining their consent.

The Clearview Defendants (Clearview AI, Inc., Hoan Ton-That, Richard Schwartz, Rocky Mountain Data Analytics LLC, and Thomas Mulcaire) (collectively, "Clearview AI") do not deny that they have violated—and are continuing to violate—BIPA. Instead, Clearview AI argues that it may ignore BIPA because the statute infringes Clearview AI's First Amendment right to free speech by inhibiting the company's ability to use, create, and disseminate information. Contrary to Clearview AI's assertions, BIPA is a content-neutral law that seeks to safeguard Illinois residents' biometric privacy. Even if BIPA incidentally burdens Clearview AI's speech, BIPA

does not violate the First Amendment because BIPA furthers substantial governmental interests unrelated to the suppression of free expression. *United States v. O'Brien*, 391 U.S. 367, 377 (1968).

BIPA furthers Illinois's substantial interest in preventing the harms that may arise from Clearview AI's unlawful collection of residents' biometric information and unconsented-to dissemination of that information to law enforcement agencies. First, Clearview AI exposes Illinois residents to police identification even as they walk down the streets or attend public events. Heightened police surveillance can, in turn, discourage free speech and association. Second, facial recognition algorithms misidentify people of color more often than white people. When used by police departments in the absence of clear guidelines, Clearview AI's facial recognition software will exacerbate systemic inequities in policing. Finally, the size and volume of Clearview AI's database, coupled with the sensitivity of the information stored in that database, increase the likelihood of recurring breaches that may jeopardize the security of millions of Illinois residents.

ARGUMENT

I. BIPA furthers Illinois's interest in protecting its residents' First Amendment rights of speech and association.

BIPA is a privacy statute that gives individuals final say over who can use their biometric information and for what purpose. In 2008, the Illinois General Assembly enacted BIPA to regulate "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5(g). As the Ninth Circuit has recognized, BIPA "protect[s] an individual's concrete interests in privacy." *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1274 (9th Cir. 2019). Because "advances in technology can increase the potential for unreasonable intrusions into personal privacy," BIPA ensures an "individual's control of information concerning his or her person." *Id.* at 1272–73.

Clearview AI collects and sells millions of Illinois residents' biometric information without

their knowledge and consent, stripping those individuals of the right to exercise control over their identities. The resulting loss of privacy and anonymity creates a chilling effect on speech and association as people fear that their views and activities, if made known to law enforcement, could invite additional surveillance, harassment, and retaliation. By preserving Illinois residents' right to control the extent to which their biometric information is disclosed to third parties, especially the police, BIPA protects those residents' First Amendment right to free speech and association.

Relying on *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011), Clearview AI argues that because BIPA discriminates based on speech content and speaker, it must survive strict scrutiny. Clearview AI Mem. of Law at 9–15. Unlike the state law at issue in *Sorrell*, which engaged in speaker and viewpoint discrimination by disfavoring marketing speech by individuals working for pharmaceutical manufacturers, 564 U.S. at 563–64, BIPA prohibits the collection and dissemination without consent of biometric information of any person, not a subset of people, and by any private entity, not just Clearview AI, *see* 740 ILCS 14/15(b), (d). *See also Turner Broad. Sys., Inc. v. F.C.C.*, 512 U.S. 622, 655 (1994). Because BIPA regulates conduct, not speech, it is constitutional so long as "a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms." *O'Brien*, 391 U.S. at 376. BIPA is constitutional because it furthers important governmental interests: namely, protecting Illinoisans' right to engage in protected First Amendment activities and guarding against misuse of facial recognition technology.[1]

A. Clearview AI facilitates unprecedented levels of police identification and surveillance.

In the hands of law enforcement agencies, Clearview AI's facial recognition software

[1] Even though strict scrutiny does not apply to BIPA, it would survive strict scrutiny because it is narrowly tailored to achieve these compelling governmental interests. *See Williams-Yulee v. Fla. Bar*, 575 U.S. 433, 444 (2015).

amplifies the government's ability to identify unknown individuals. The company scrapes images of individuals from various websites, including Facebook, Twitter, and Instagram, and creates "faceprints" based on those images. A faceprint, like a fingerprint, maps the physical characteristics that make each person unique. When a police officer submits an image of an unidentified suspect—or a "probe image"—to Clearview AI's software, the company's facial recognition algorithm generates a faceprint from the probe image, compares that faceprint with more than three billion existing faceprints in the Clearview AI database, and proposes possible matches.[2] Clearview AI also directs the police officer to the websites from which the images were scraped. These source websites may reveal the names and other personal information about the individuals Clearview AI suggests as matches.

Over 3,100 law enforcement agencies in the United States use Clearview AI's facial recognition software.[3] Police departments, intelligence agencies, immigration enforcement authorities, and any other users of Clearview AI's software may be able to "identify [an] individual in any of the . . . hundreds of millions of photos" uploaded to the Internet each day. *See Patel*, 932 F.3d at 1273. The government may identify others "who are present in the photo" as well. *See id.* If taken at a political rally, a church service, or an abortion clinic, an individual's photo could unveil to the government "a wealth of detail about her familial, political, professional, religious, and sexual associations." *See United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). Indeed, photos posted on social media often have geotags, captions, and "likes," revealing a person's locational history, preferences, and relationships.

The surveillance practices of other countries illustrate how far governments may be willing

[2] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times, Jan. 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[3] Kashmir Hill, *Your Face Is Not Your Own*, N.Y. Times, Mar. 8, 2021, https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html.

to deploy facial recognition technology to monitor and track individuals. In China, a network of surveillance cameras equipped with facial recognition software can single out individuals from a crowd, analyze their faces, and trace their movements across a city.[4] The Chinese government's use of real-time facial recognition is so widespread that Hong Kong democracy activists covered their faces during a series of protests to avoid being identified by the state.[5] In the United Kingdom, there are "eye[s] in the sky" scanning faces of individuals throughout the London streets to determine whether any of those individuals belongs to a police watch list.[6]

Real-time facial identification is not a remote concern for Americans, including those in Illinois. The Chicago Police Department once proposed in its application for a Department of Homeland Security grant to deploy facial recognition technology on surveillance cameras in and around Chicago.[7] Similarly, the Detroit Police Department indicated in its facial recognition policy that the department "may connect the face recognition system to *any* interface that performs live video, including cameras, drone footage, and body-worn cameras."[8] Clearview AI has already begun embedding its facial recognition software into surveillance cameras and wearable smart devices, providing police departments across the country with an option for acquiring real-time identification capability.[9]

---

[4] Simon Denyer, *Beijing Bets on Facial Recognition in a Big Dive for Total Surveillance*, Washington Post, Jan. 7, 2018, https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance.

[5] Paul Mozur, *In Hong Kong Protests, Faces Become Weapons*, N.Y. Times, Jul. 26, 2019, https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html.

[6] Philip Chertoff, *Facial Recognition Has Its Eye on the U.K.*, Lawfare, Feb. 7, 2020, https://www.lawfareblog.com/facial-recognition-has-its-eye-uk.

[7] Clare Garvie & Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, Center on Privacy & Technology, May 16, 2019, https://www.americaunderwatch.com.

[8] *Id.*

[9] Dave Gershgorn, *Glasses Equipped With Facial Recognition Are Coming*, OneZero, May 22, 2020, https://onezero.medium.com/glasses-equipped-with-facial-recognition-are-coming-ac2ccfe2795a; Martin Kaste, *Real-Time Facial Recognition Is Available, But Will U.S. Police Buy It?*, NPR, May 10, 2018,

B. Clearview AI's conduct unlawfully chills Illinois residents' expressive and associational activities.

The ongoing partnership between Clearview AI and law enforcement exposes Illinois residents to the heightened threat of government surveillance and creates a chilling effect on those residents' First Amendment activities. For one, Clearview AI's extraction of individuals' biometric information from the Internet and dissemination of that information to police departments in the absence of those individuals' knowledge and consent can chill expressive activities online. A website user may well weigh the benefits of every movement on the Internet—whether it be commenting on a political subject or endorsing a controversial public figure—against the costs of Clearview AI's data scraping and the government's subsequent use of that data. As the Supreme Court has noted, "[f]ear or suspicion that one's speech is being monitored by a stranger . . . can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas." *Bartnicki v. Vopper*, 532 U.S. 514, 533 (2001) (quotation omitted). Similarly, individuals may be deterred from attending political rallies or participating in public protests out of fear that police might identify them from a crowd, track their whereabouts, and use that information against them. Even police and government officials recognize that facial recognition is "a form of surveillance" that "can adversely impact freedom, creativity, and self-development."[10]

The Supreme Court has repeatedly recognized privacy and anonymity as core First Amendment values that enable individuals to express ideas and seek membership in groups without fear of retaliation. In *NAACP v. Alabama*, for example, the Court stressed this "vital relationship between freedom to associate and privacy in one's associations." 357 U.S. 449, 462

---

https://www.npr.org/2018/05/10/609422158/real-time-facial-recognition-is-available-but-will-u-s-police-buy-it.

[10] *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field*, International Justice and Public Safety Network, at 17 (June 30, 2011), https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf.

(1958). The Court held that the NAACP could not be compelled by state law to disclose the identities of its members because such disclosure, "particularly where a group espouses dissident beliefs," would restrain the members' freedom of association and expose them to "economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility." *Id.*; *see also Bates v. City of Little Rock*, 361 U.S. 516, 527 (1960) (holding that cities cannot compel organizations to disclose membership lists because doing so would deter free association).

The Supreme Court has underscored the particular importance of privacy and anonymity to minority groups. In *Talley v. California*, the Court struck down a city ordinance that prohibited anonymous handbills, noting that throughout history, "persecuted groups . . . have been able to criticize oppressive practices and laws either anonymously or not at all." 362 U.S. 60, 64 (1960). Similarly, in *McIntyre v. Ohio Elections Commission*, the Court recognized anonymous speech as "an honorable tradition of advocacy and of dissent" that "exemplifies the purpose behind the Bill of Rights[] and of the First Amendment[,]" which is "to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society." 514 U.S. 334, 357 (1995). "Anonymity is a shield from the tyranny of the majority." *Id.*

Illinois has a substantial interest in protecting the First Amendment activities of its residents, especially those who support unpopular ideas in today's increasingly polarized political climate.[11] As the Supreme Court has emphasized, there is "substantial evidence of past and present hostility from private persons and government officials" against members of minority groups, "subject[ing] those persons identified to the reasonable probability of threats, harassment or reprisals." *Brown v. Socialist Workers '74 Campaign Comm.*, 459 U.S. 87, 101–02 (1982); *cf.*

[11] *See* Levi Boxell et al., Abstract, *Cross-Country Trends in Affective Polarization*, Working Paper 26669, National Bureau of Economic Research, rev. June 2020, https://www.nber.org/papers/w26669.

Buckley v. Valeo, 424 U.S. 1, 71 (1976) ("[T]he damage done by disclosure to the associational interests of the minor parties and their members . . . could be significant . . . to the point where the movement cannot survive."). Consequently, when people realize that their privacy and anonymity have been compromised, "they readily conform their behavior—expressing opinions when they are in the majority, and suppressing them when they're not."[12]

Clearview AI argues that individuals have no privacy interest in photographs they post on the Internet. This argument is wrong for two reasons. First, the Supreme Court has made clear that individuals retain their right to remain anonymous even where they have voluntarily exposed their faces to the public. *See, e.g.*, *Watchtower Bible and Tract Society of New York v. Stratton*, 536 U.S. 150, 166–67 (2002) (holding unconstitutional a village ordinance requiring canvassers to identify themselves in a permit and to display that permit upon demand). *Watchtower* affirms that individuals have the right to remain anonymous even as they walk down the streets or attend public protests. *Id.*; *see also Buckley v. Am. Constitutional Law Found., Inc.*, 525 U.S. 182, 200 (1999) (holding that a state statute requiring petition circulators to wear identification badges violated the circulators' First Amendment right to free speech); *McIntyre*, 514 U.S. at 348 ("[T]he identity of the speaker is no different from other components of the document's content that the author is free to include or exclude.").

The same reasoning applies to the digital space. "Although the Internet is the latest platform for anonymous speech, online speech stands on the same footing as other speech." *In re Anonymous Online Speakers*, 661 F.3d 1168, 1173 (9th Cir. 2011). Indeed, a social media user whose photo may be visible to others on the Internet would not reasonably anticipate her facial geometry to be measured from her photo, scanned into a database, analyzed to create a faceprint,

[12] Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 Journalism & Mass Communication Quarterly 307 (Mar. 8, 2016).

and then sold to the police to identify her.

It is increasingly difficult to live a full life without an online presence. Clearview AI's unlawful scraping and disseminating of biometric information chills expressive and associational activities such as joining an online group that organizes pick-up soccer games, or maintaining a LinkedIn profile. Posting one's photo online is not the same as allowing someone else to purloin that photo and use it for purposes that may be inimical to the photo's subject.

Second, Clearview AI's argument that people who publish their photos online assume the risk of third parties harvesting those photos, s*ee* Clearview AI Mem. of Law at 12, 15 16, 17, fails to address an entire group of individuals who did not share their photos in the first place. Many people appear in photos online because someone else—a friend, a family member, or even a complete stranger—uploaded those photos either with or without their informed consent. Indeed, it is virtually impossible to exist in society without appearing somewhere online, even if one does not post anything to the Internet oneself.

The relevant inquiry here is thus not whether a person has voluntarily appeared in public—doing so is a life necessity—but rather what types of harm the loss of privacy and anonymity will inflict on that person. One such harm that the Supreme Court has consistently warned against in its line of First Amendment cases—and one that Illinois has a substantial interest in protecting its residents against—is the abridgment of free speech and association.[13]

[13] Clearview AI contends that BIPA is unconstitutionally overbroad because it would be too difficult for Clearview to comply with BIPA. Clearview AI Mem. of Law at 16–17. BIPA is not overbroad in scope; it regulates the use of biometric information. Clearview AI essentially argues that BIPA interferes with its business model, but BIPA does not interfere with legitimate business models. *See, e.g.*, Order re Final Approval, Attorneys' Fees and Costs, and Incentive Awards at 3, *In re Facebook Biometric Info. Privacy Litig.*, No. 15-cv-03747-JD (N.D. Cal. Feb. 26, 2021).

II. BIPA furthers Illinois's interest in protecting its residents from police misuse of facial recognition technology.

Police departments across the country, including those in Illinois, increasingly rely on facial recognition technology to assist their investigations. Clearview AI, for instance, boasts that its tool yields "high-quality leads with fewer resources expended" to "accurately and rapidly identify suspects, persons of interest, and victims."[14] A majority of Clearview AI's clients is indeed law enforcement and government agencies.[15] In Illinois alone, Clearview AI has had at least 105 customers, including the Chicago Police Department.[16]

Bias, however, is baked into facial recognition technology. Multiple studies have demonstrated that artificial intelligence algorithms used in facial recognition applications tend to discriminate based on classes like race, gender, and age. Moreover, like any other surveillance tool, facial recognition technology can be misused. When individual police officers have the unconstrained power to determine which probe images to input and how to interpret the outputs that facial recognition produces, the likelihood of misuse increases dramatically. As Clearview AI continues to collect and disseminate Illinois residents' biometric information to law enforcement without those residents' informed consent, more people will be exposed to the risk of police misidentification. Therefore, Illinois has a substantial interest in protecting its residents, particularly women and people of color, from police misuse of facial recognition technology.

---

[14] *Law Enforcement*, Clearview AI, https://clearview.ai/law-enforcement (last visited July 6, 2021).
[15] A leaked client list in 2020 showed that Clearview AI provided services to a number of private entities, despite its claims to the contrary. *See* Sara Morrison, *The world's scariest facial recognition company is now linked to everybody from ICE to Macy's*, Vox, Feb. 28, 2020, https://www.vox.com/recode/2020/2/26/21154606/clearview-ai-data-breach.
[16] *See* Ryan Mac et al., *Clearview AI Has Promised to Cancel All Relationships with Private Companies*, BuzzFeed News, May 7, 2020, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies; Tom Schuba, *CPD using controversial facial recognition program that scans billions of photos from Facebook, other sites*, Chicago Sun-Times, Jan. 29, 2020, https://chicago.suntimes.com/crime/2020/1/29/21080729/Clearview AI-ai-facial-recognition-chicago-police-cpd.

A. Police use Clearview AI's software without implementing best practices to mitigate the unreliability of facial recognition technology.

Several studies have confirmed that algorithmic biases in facial recognition more often result in the erroneous matching of images of individuals belonging to certain racial, gender, and age groups. The National Institute of Standards and Technology (NIST), for example, found that a majority of the facial recognition algorithms it tested misidentify people of color more often than white people. When tested on domestic law enforcement images, facial recognition algorithms yielded "the highest false positives . . . in American Indians, with elevated rates in African American and Asian populations[.]"[17] Moreover, facial recognition algorithms tended to be less accurate on the elderly and children than on middle-aged adults.

Although a false positive match in a law enforcement context "could lead to a false accusation, detention[,] or deportation,"[18] police departments continue to use Clearview AI's facial recognition software without imposing accuracy standards. Indeed, there is no evidence of Clearview AI's law enforcement clients requiring the company to subject its facial recognition algorithms to independent, rigorous, and regular testing to detect potential bias. Although Clearview AI insists that its algorithm is "100% accurate" and "consistent across all racial and demographic groups,"[19] Clearview AI's refusal to permit facial recognition technology experts to test its algorithm speaks volumes about its accuracy. Clearview AI has not subjected its technology to a robust peer review process, such as the NIST Facial Recognition Vendor Test program, for

---

[17] Patrick Grother et al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NIST, U.S. Department of Commerce, December 2019, at 2, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[18] *Id.* at 5.

[19] Thomas Macaulay, *Clearview AI's false claims of accuracy increase the dangers of its face recognition software*, TNW, Feb. 11, 2020, https://thenextweb.com/news/Clearview AI-ais-false-claims-of-accuracy-increase-the-dangers-of-its-face-recognition-software. *See also* Richard Adhikari, *ACLU Blasts Clearview AI's Facial Recognition Accuracy Claims*, ECT News Network, Feb. 14, 2020, https://www.technewsworld.com/story/86512.html.

validation.[20]

The lack of best practices guiding individual police officers' use of facial recognition technology further exacerbates the unreliability problem. There are, for example, "no rules" concerning what probe images police can submit to facial recognition applications to generate investigative leads.[21] Consequently, police officers can submit probe images of varying quality, ranging from "low-quality surveillance camera stills, social media photos with filters, and scanned photo album pictures" to "computer-generated facial features, [] composite or artist sketches," and a photo of "a suspect's celebrity doppelganger."[22] Because cameras have traditionally been designed to best capture light skin, photos of dark-skinned people are typically of lower quality to begin with.[23] Police officers routinely doctor probe photos, employing 3D modeling software in an attempt to rotate or complete faces that are otherwise turned away from the camera.[24] The New York City Police Department even used Google to search for an image of a "Black Male Model," whose lips were then cut and pasted into a probe image in which the suspect's mouth was obstructed.[25] Police officers' use of questionable—or fabricated—probe images produces unreliable results. "Photos that are pixelated, distorted, or of partial faces provide less data for a face recognition system to analyze than high-quality, passport-style photos, increasing room for error."[26] BIPA protects Illinois residents' choice to withhold their photographs from a database that is searched using such unreliable methods.

---

[20] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, supra note 1.
[21] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, Center on Privacy & Technology, Mar. 16, 2019, https://www.flawedfacedata.com/ (*Garbage In, Garbage Out*).
[22] *Id.*
[23] *See* Sarah Lewis, The Racial Bias Built Into Photography, N.Y. Times, Apr. 25, 2019, https://www.nytimes.com/2019/04/25/lens/sarah-lewis-racial-bias-photography.html.
[24] *Garbage In, Garbage Out*, supra note 21.
[25] *Id.*
[26] *Id.*

B. Law enforcement's reliance on Clearview AI puts Illinois residents at increased risk of misidentification and false arrest.

The costs of police misuse of facial recognition technology are real and consequential. In January 2020, police officers investigating a watch theft wrongfully arrested Robert Julian-Borchak Williams, a Black man from Michigan, based on a flawed match established by facial recognition software. Police in Detroit had used a blurry still photograph from a surveillance video as a probe image to identify the person who appeared to be the suspect. When the facial recognition software identified Williams as a match, police arrested Williams and detained him for thirty hours. At a court hearing, prosecutors dropped the charges against Williams because he had an airtight alibi.[27]

Williams is not the only person who was arrested for a crime he did not commit. Two other Black men—Nijeer Parks and Michael Oliver—were also wrongfully arrested based on false facial recognition matches.[28] Unfortunately, these are just the known cases of wrongful arrests resulting from police use of flawed facial recognition technology. It is impossible to know how many more individuals have been wrongly arrested due to facial recognition technology because police typically do not inform arrested people that they were identified by facial recognition technology.

Even though police insist that they use facial recognition technology in criminal investigations to generate "leads only," there is no guarantee that police pursue corroborating evidence before arresting individuals identified as possible matches.[29] In the absence of policies and procedures mitigating the risk of police misuse of facial recognition technology, what happened to Williams, Parks, and Oliver may not be a distant reality for Illinois residents.

---

[27] Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. Times, June 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.
[28] Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. Times, Dec. 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.
[29] *Garbage In, Garbage Out*, supra note 21.

III. BIPA furthers Illinois's interest in ensuring the security of its residents' sensitive personal information.

Clearview AI is especially dangerous because the company collects and handles information that is "unlike other unique identifiers . . . used to access finances or other sensitive information." 740 ILCS 14/5(c). Unlike passwords or social security numbers, for example, faceprints are unique to each person and cannot simply be changed if stolen. Hackers who gain unauthorized access to Clearview AI's database might access not only individuals' biometric information, but also the source websites where Clearview AI scraped the photographs of individuals, thus discovering names and other personal information. As Clearview AI is well aware, its stockpile of billions of faceprints is a holy grail for malicious actors on the Internet.

Despite the volume and sensitivity of the data stored in its database, Clearview AI does not have adequate data protection measures in place. At one point, "a misconfigured server" exposed Clearview AI's "internal files, apps and source code for anyone on the internet to find."[30] In 2020, a malicious actor breached Clearview AI's security system and leaked the identity of Clearview AI's customers. Clearview AI simply stated that "data breaches are a part of life."[31] Clearview AI's cavalier response does not portend well for the future.

Clearview AI's insufficient data security places millions of Illinois residents at increased risk of hacking, identity theft, financial fraud, stalking, and harassment. Although Clearview AI states that individuals can request to opt out of its database, this option is futile when most people do not know that Clearview AI has collected, used, and retained their biometric information in the

[30] Zack Whittaker, *Security lapse exposed Clearview AI source code*, TechCrunch, Apr. 16, 2020, https://techcrunch.com/2020/04/16/clearview-source-code-lapse/.
[31] Jordan Valinsky, *Clearview AI Has Billions of Our Photos. Its Entire Client List Was Just Stolen*, CNN Business, Feb. 26, 2020, https://www.cnn.com/2020/02/26/tech/Clearview AI-ai-hack/index.html.

first place. Nor does Clearview AI honor all opt-out requests it receives.[32] Even where it does, the company provides no guarantee that the photographs of those who have opted out will not be re-scraped in the future.

Given "the sensitivity of biometric information and the risk of identity theft[,]" *Bryant v. Compass Group USA, Inc.*, 958 F.3d 617, 626 (7th Cir. 2020), Illinois has a substantial interest in regulating actors like Clearview AI and ensuring "the public welfare, security, and safety[.]" 740 ILCS 14/5(g). For millions of Illinois residents, BIPA affords "the opportunity to make informed choices about to whom and for what purpose they will relinquish control of that information." *Bryant*, 958 F.3d at 626. BIPA protects Illinois residents from theft of their personal biometric information. BIPA furthers substantial governmental interests unrelated to the suppression of free expression and therefore survives intermediate scrutiny.

CONCLUSION

For the reasons set forth above, the Center urges the Court to deny Clearview AI's motion to dismiss.

Dated: July 8, 2021

/s/ Rachel L. Fried
Rachel L. Fried (pro hac vice pending)
David C. Vladeck
Civil Litigation Clinic
Georgetown University Law Center
600 New Jersey Avenue, NW
Washington, D.C. 20001
(202) 662-9540

Craig B. Futterman
Edwin F. Mandel Legal Aid Clinic
6020 South University Avenue
Chicago, IL 60637
(773) 702-9611

[32] On May 16, 2020, Clare Garvie of the Center submitted a request to Clearview AI's Privacy Team to access any information the company has about her and pursue, if necessary, the right to rectification of that data. The Clearview AI Privacy Team responded on April 2, 2020 that the company is unable to process Ms. Garvie's request "[d]ue to a high volume of requests and security concerns[.]"

futterman@uchicago.edu

Counsel for Amicus Center on Privacy & Technology